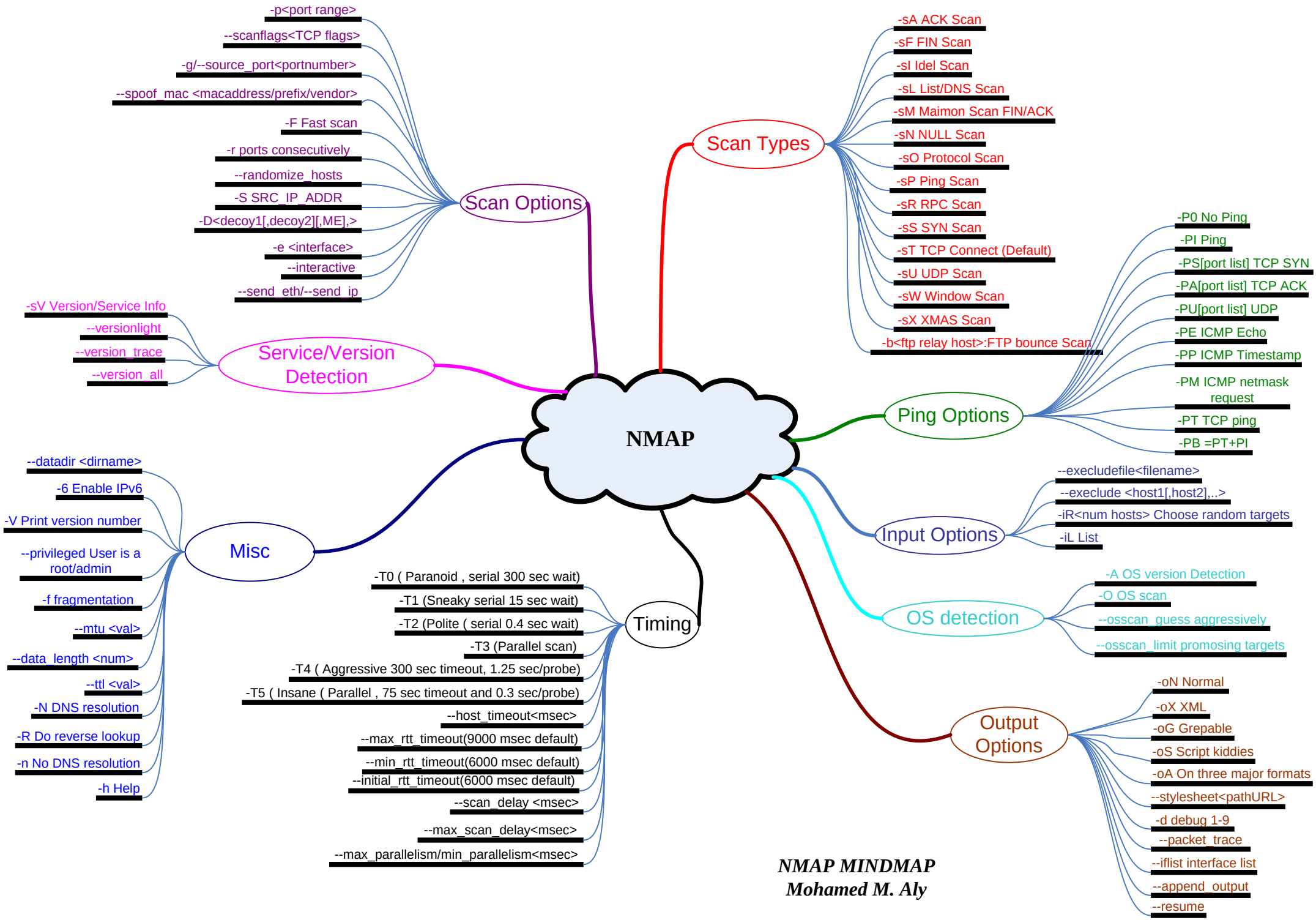
NMAP
Scan Options
-p<port range>
--scanflags<TCP flags>
-g/--source_port<portnumber>
--spoof_mac <macaddress/prefix/vendor>
-F Fast scan
-r ports consecutively
--randomize_hosts
-S SRC_IP_ADDR
-D<decoy1[,decoy2][,ME],>
-e <interface>
--interactive
--send_eth/--send_ip
Scan Types
-sA ACK Scan
-sF FIN Scan
-sI Idel Scan
-sL List/DNS Scan
-sM Maimon Scan FIN/ACK
-sN NULL Scan
-sO Protocol Scan
-sP Ping Scan
-sR RPC Scan
-sS SYN Scan
-sT TCP Connect (Default)
-sU UDP Scan
-sW Window Scan
-sX XMAS Scan
-b<ftp relay host>:FTP bounce Scan
Ping Options
-P0 No Ping
-PI Ping
-PS[port list] TCP SYN
-PA[port list] TCP ACK
-PU[port list] UDP
-PE ICMP Echo
-PP ICMP Timestamp
-PM ICMP netmask request
-PT TCP ping
-PB =PT+PI
Service/Version Detection
-sV Version/Service Info
--versionlight
--version_trace
--version_all
Misc
--datadir <dirname>
-6 Enable IPv6
-V Print version number
--privileged User is a root/admin
-f fragmentation
--mtu <val>
--data_length <num>
--ttl <val>
-N DNS resolution
-R Do reverse lookup
-n No DNS resolution
-h Help
Timing
-T0 (Paranoid , serial 300 sec wait)
-T1 (Sneaky serial 15 sec wait)
-T2 (Polite (serial 0.4 sec wait)
-T3 (Parallel scan)
-T4 (Aggressive 300 sec timeout, 1.25 sec/probe)
-T5 (Insane (Parallel , 75 sec timeout and 0.3 sec/probe)
--host_timeout<msec>
--max_rtt_timeout(9000 msec default)
--min_rtt_timeout(6000 msec default)
--initial_rtt_timeout(6000 msec default)
--scan_delay <msec>
--max_scan_delay<msec>
--max_parallelism/min_parallelism<msec>
Input Options
--execludefile<filename>
--execlude <host1[,host2],..>
-iR<num hosts> Choose random targets
-iL List
OS detection
-A OS version Detection
-O OS scan
--osscan_guess aggressively
--osscan_limit promosing targets
Output Options
-oN Normal
-oX XML
-oG Grepable
-oS Script kiddies
-oA On three major formats
--stylesheet<pathURL>
-d debug 1-9
--packet_trace
--iflist interface list
--append_output
--resume
NMAP MINDMAP
Mohamed M. Aly